UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/774,079	02/06/2004	Shehzad T. Merchant	2717P176	7139

8791 7590 05/24/2010

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
POPHAM, JEFFREY D	
ART UNIT	PAPER NUMBER
2437	
MAIL DATE	DELIVERY MODE
05/24/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/774,079	MERCHANT ET AL.	
	Examiner	Art Unit	
	JEFFREY D. POPHAM	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 February 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 July 2009* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Remarks

Claims 1-51 are pending.

Response to Arguments

1. Applicant's arguments filed 2/3/2010 have been fully considered but they are not fully persuasive.

With respect to the amendment to claim 10, adding "the client communicates to the authenticator from a user station", this user station is not actually part of the network system of claim 10. Rather, this user station can communicate with entities in the network system. Therefore, as the user station is not actually part of the network system, it does not have any bearing on the network system with respect to the 101 rejection (even if the user station is described in the specification as being hardware).

Applicant argues that "Neither Stewart nor Choi disclose that the location information indicates the association between a particular port of the network switch and the physical location of an edge device or a wired user station associated with the particular port of the network switch." Page 7, lines 14-16 states that "When the location information is associated with a particular port, it can indicate the physical location of the edge device or wired user station 18a-b connected to the port." Using this definition, Stewart can be seen as teaching the location information indicating an association between a port of the switch and an edge device, as Stewart teaches edge devices providing location information, such edge devices being connected to the switch via a port. However, for

purposes of completeness, the rejection includes Liming in order to specifically show a location of the switch itself (where the ports on the network switch of Stewart resides, therefore, being the same location information for both the port on the switch as well as the switch itself).

Applicant argues that "Stewart and Torvinen are silent on the subject of network administrator, and Stewart and Torvinen are silent on the subject of a policy table". However, each of a network administrator and a policy table do not have to be recited with the same exact language. As an example, a network administrator is often referred to as a network manager. As for a policy table, this can be any table that provides for some form of policy and policy-based decisions. As can be seen in Torvinen, a network operator can create, update, and manage groups and the corresponding restrictions therefore (paragraphs 54 and 58, for example). This network operator is a network administrator within Torvinen, as the network operator administers the network. Furthermore, Torvinen describes other users being able to create, update, and manage groups by using mobile devices. In this situation, the user may be seen to correspond to a network administrator as the user is administering the group on the network. The restrictions correspond to policies, as they identify such restrictions as location and proficiency levels. Torvinen may not explicitly describe a table for such policies, however, Stewart does describe a policy table, including such information as access method, access level, identification information, and network provider identification. In this situation, access level may be seen to correspond to the restrictions of Torvinen, as the restrictions of Torvinen describe

an access level. Therefore, the combination of Stewart in view of Torvinen discloses a network administrator that can create and update a policy table.

Applicant argues that "Neither Stewart nor Choi disclose a network management system that can optionally connect to the network or directly connect to the authentication server and one or more switches. A review of both reference confirm that these network management features are not disclosed, considered singly or in combination." However, in reviewing Torvinen, this element is found therein, when used in combination with Stewart. In Torvinen, the management component may reside in all servers such as servers 204-208 and 212 in figure 2 (paragraph 48 teaches this). As all of these management components are connected via the network, they are connected through the network. However, since each management component is provided on the server itself, there is a direct connection between the management component and the server. As discussed previously in the rejections using Stewart, any of the entities in Stewart, such as AP, switch, MIB, etc. may correspond to the authentication server of the claims. Therefore, as each of those entities may correspond to the authentication server, and Torvinen teaches providing the management component on each server, the combination clearly teaches both directly connecting to each server via its own management component (which bypassing the network, as it is within the same device) as well as communication between the management components and/or servers via the network.

It is noted that in the rejections below, some of the grounds of rejection have been modified due to the amendments. As an example, claim 1 was

amended such that Choi is no longer required in the rejection. However, claim 1 was also amended such that Liming is required in the rejection. This is one example, however, other grounds of rejection have been changed due to the amendment as well. It should be readily understood that these changes in grounds of rejection were necessitated by the most recent amendment.

Claim Objections

2. Claims 10, 27, 29, 30, 32, 33, and 36 are objected to because of the following informalities:

- The final limitation of claim 10 refers to "the network administrator" before any such administrator has been set forth in the claim. For purposes of prior art rejection, “the network administrator” has been construed as “a network administrator”.
- The authentication server limitation of claim 27 states “based on the corresponding identify”, where "identify" should read "identity".
- Each of claims 29, 30, 32, and 33 refer to “the network switch”. However, claim 27, from which these claims depend, has been amended to refer to “one or more network switches”. For purposes of prior art rejection, “the network switch” has been construed as “the one or more network switches”.
- Claim 36 refers to a “RADIUS serve”, which should apparently read “RADIUS server”.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 10, 17-19, 21-24, and 26 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 10 is directed to a network system comprising a network, an authenticator, a data structure, an authentication server, and a network manager. None of these entities are inherently physical. A network is a connection of entities. An authenticator is described in the application as being located at a switch or edge device. Therefore, the authenticator can be merely software. A data structure is data by its very basis. An authentication server "can be included as a component in one or more of the switches" (page 8, lines 28-30). This is also shown in claim 20. The only interpretation one can make of this is that an authentication server need not be a physical entity, but may be logical (e.g. program code). Therefore, the authentication server (and broader server) need not include physical components. Furthermore, a server is generally defined as being a device or a program. A network manager is described in the specification, such that "The network manager 20 can be a server running an application" (page 6, lines 14-15). Therefore, the interpretation taken for a network manager is equivalent to that of a server. All of the entities of claim 10 could be hardware, software/logical, or a combination thereof. Therefore, claim 10 fails to fall in one

of the statutory categories of invention, since it is not a process, apparatus, article of manufacture, or composition of matter. Claims 11-16, 20, and 25 provide physical elements (edge devices, client devices, and network switches) and are, therefore, statutory. Claims 17-19, 21-24, and 26, however, do not fix the issue, and are rejected for the same reasons as claim 10.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 2, 4-6, 8, 9, 46, and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart (U.S. Patent 6,732,176).

Regarding Claim 1,

Stewart discloses a method of controlling access to a network comprising:

Requesting an identity from a mobile client attempting to connect to the network (Column 10, line 64 to Column 11, line 16);

Receiving the identity (Column 10, line 64 to Column 11, line 16);

Associating location information corresponding to the client with the identity (Column 11, lines 17-53);

Authenticating the identity (Column 9, lines 28-47; Column 12, line 30 to Column 13, line 10; and Column 18, lines 1-25);

Comparing the location information against a policy designating locations, if any, at which the client is permitted to connect to the network (Column 11, lines 28-53; and Column 16, lines 38-64; determining access levels based on location);

Deciding whether to grant or deny client access to the network based on the authenticity of the identity and comparison of the location information (Column 11, lines 28-53; Column 12, lines 47-63; and Column 16, lines 15-55; granting differing levels of access based on identification information as well as geographic information); and

Providing a network switch including a plurality of ports for connecting the edge devices to a network (Figures 2-3; and Column 9, lines 52-64);

But does not appear to explicitly disclose that the location information indicates the location of a network switch to which the client is attempting to connect, and the location information indicates the association between a particular port of the network switch and the physical location of an edge device or a wired user station associated with the particular port of the network switch.

Liming, however, discloses that the location information indicates the location of a network switch to which the client is

attempting to connect, and the location information indicates the association between a particular port of the network switch and the physical location of an edge device or a wired user station associated with the particular port of the network switch (Paragraphs 159, 165, and 181; location of the switch being connected to, for example). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the location context system of Liming into the distributed network access system of Stewart in order to allow the system to associate location information with the client even when the other devices cannot provide such location information, thereby extending the system to be able to be used when the client connects directly to a switch and/or when the other devices between the client and switch do not have any means to associate location information with the client.

Regarding Claim 2,

Stewart as modified by Liming discloses the method of claim 1, in addition, Stewart discloses passing the identity and the location information to an authentication server, wherein the authentication server performs the steps of authenticating, comparing, and deciding (Column 10, line 64 to Column 11, line 16; and Column 14, lines 40-56; the authentication server could be the MIB, for example).

Regarding Claim 4,

Stewart as modified by Liming discloses the method of claim 1, in addition, Stewart discloses that the identity includes information selected from the group consisting of a user name, a user password, a certificate, a MAC address, a shared encryption key, a smart card identifier, and any combination of the foregoing information (Column 10, lines 53-63).

Regarding Claim 5,

Stewart as modified by Liming discloses the method of claim 1, in addition, Stewart discloses that the client is a user station capable of connecting to the network through an access point (Column 10, line 64 to Column 11, line 16).

Regarding Claim 6,

Stewart as modified by Liming discloses the method of claim 1, in addition, Stewart discloses that the client is a wired device capable of connecting to the network through an Ethernet switch port (Column 5, lines 2-24; Column 6, lines 40-59; and Column 9, lines 48-64).

Regarding Claim 8,

Stewart as modified by Liming discloses the method of claim 1, in addition, Liming discloses that the location information indicates the location of a network switch to which the client is attempting to connect (Paragraph 159).

Regarding Claim 9,

Stewart as modified by Liming discloses the method of claim 1, in addition, Stewart discloses that the location information indicates the location of an edge device for connecting the client to the network (Column 11, lines 17-27).

Regarding Claim 46,

Stewart as modified by Liming discloses the method of claim 1, in addition, Stewart discloses that the mobile client is associated with newly located access point upon authenticating the identity of the mobile client and determining, by comparing updated location information corresponding to the mobile client against the policy, that the mobile client is still authorized to access the network (Column 9, lines 28-47; Column 10, lines 25-37; Column 12, line 30 to Column 13, line 10; Column 14, line 57 to Column 15, line 15; and Column 18, lines 1-25).

Regarding Claim 48,

Stewart as modified by Liming discloses the method of claim 8, in addition, Liming discloses that the location information indicates the location of a port of a network switch to which the client is attempting to connect (Paragraphs 159, 165, and 181).

5. Claims 3 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Liming, further in view of Funk (Funk Software,

"Comprehensive RADIUS/AAA Solution for the Global Enterprise", 2/22/2003, pp. 1-6).

Regarding Claim 3,

Stewart as modified by Liming does not explicitly disclose that the authentication server is a RADIUS server.

Funk, however, discloses that the authentication server is a RADIUS server (Pages 1-6). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the AAA system of Funk into the distributed network access system of Stewart as modified by Liming in order to allow the system to centralize security and access controls, such as authentication, authorization, and accounting, manage the busiest of networks, scale to accommodate growing networks, and/or to provide high reliability and uptime.

Regarding Claim 7,

Stewart as modified by Liming does not explicitly disclose using a mechanism selected from the group comprising TLS, TTLS, MD5, EAP-TLS, and any combination of the foregoing to authenticate the identity.

Funk, however, discloses using a mechanism selected from the group comprising TLS, TTLS, MD5, EAP-TLS, and any combination of the foregoing to authenticate the identity (Page 3). It would have been obvious to one of ordinary skill in the art at the

time of applicant's invention to incorporate the AAA system of Funk into the distributed network access system of Stewart as modified by Liming in order to allow the system to centralize security and access controls, such as authentication, authorization, and accounting, manage the busiest of networks, scale to accommodate growing networks, and/or to provide high reliability and uptime.

6. Claims 10, 12-16, 18, 19, 21, 22, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Torvinen (U.S. Patent Application Publication 2005/0149443).

Regarding Claim 10,

Stewart discloses a network system comprising:

A network (Figure 1);

An authenticator for requesting an identity from a client and for associating location information corresponding to the client with the identity, wherein the client communicates to the authenticator from a user station (Column 10, line 64 to Column 11, line 27);

A data structure, accessible by an authentication server, associating identities of clients with their authorized access locations (Column 7, line 24 to Column 8, line 3; Column 12, line 55 to Column 13, line 11; Column 15, lines 17-28; and Column 16, lines 38-55; data structure stored on the MIB or other entity

comprising information regarding and associating access levels, locations, identities, providers, etc., for example);

The authentication server, upon receiving the identity and associated location information from the authenticator, deciding whether to grant or deny client access to the network by accessing the data structure and determining that the location information corresponding to the client specifies a location that is one of the authorized access locations, if any, for the client as maintained in the data structure (Column 9, lines 28-47; Column 12, line 30 to Column 13, line 10; Column 14, lines 40-56; Column 16, lines 38-55; and Column 18, lines 1-25; the authentication server may be any entity accessing the data structure for the purpose of authentication and location-based access; various embodiments of Stewart show the AP, network providers, and/or MIB providing portions of or the entirety of the authentication server); and

A policy table in the authentication server (Column 7, line 24 to Column 8, line 3; Column 12, line 55 to Column 13, line 11; Column 15, lines 17-28; and Column 16, lines 38-55);

But does not explicitly disclose a network manager comprising an application running on a server, wherein the application permits a network administrator to create and update the policy table in the authentication server.

Torvinen, however, discloses a network manager comprising an application running on a server, wherein the application permits a network administrator to create and update the policy table in the authentication server (Paragraphs 27-28, 30, 42, 45, 54, and 58; a management component, logic, or application that allows a network operator or user in control of a group to create and maintain a data structure including a region of interest and/or proficiency level that is allowed to join the group in order to perform particular actions or acquire particular data associated with the group, for example). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the conditional group access system of Torvinen into the distributed network access system of Stewart in order to allow various groups to be formed, by network operators and normal users alike, such that groups may be based upon the location of the device, device capabilities, user capabilities or subscriptions, etc., thereby providing additional beneficial services to users by allowing them to communicate with other users that are in the same location and/or have the same interests.

Regarding Claim 12,

Stewart as modified by Torvinen discloses the system of claim 10, in addition, Stewart discloses that the authenticator

resides in an edge device (Column 10, line 64 to Column 11, line 16).

Regarding Claim 13,

Stewart as modified by Torvinen discloses the system of claim 10, in addition, Stewart discloses an edge device for connecting a user station to a network switch (Figures 2-3).

Regarding Claim 14,

Stewart as modified by Torvinen discloses the system of claim 13, in addition, Stewart discloses that the edge device is a wireless access point (Column 10, line 64 to Column 11, line 16).

Regarding Claim 15,

Stewart as modified by Torvinen discloses the system of claim 14, in addition, Stewart discloses that the user station capable of connecting to the network through the access point (Column 5, lines 1-14; and Column 10, line 64 to Column 11, line 16).

Regarding Claim 16,

Stewart as modified by Torvinen discloses the system of claim 10, in addition, Stewart discloses that the client is a wired device capable of connecting to a network switch through an Ethernet port (Column 5, lines 2-24; Column 6, lines 40-59; and Column 9, lines 48-64).

Regarding Claim 18,

Stewart as modified by Torvinen discloses the system of claim 10, in addition, Stewart discloses that the location information indicates the location of an edge device for connecting the client to the network (Column 10, line 64 to Column 11, line 27).

Regarding Claim 19,

Stewart as modified by Torvinen discloses the system of claim 18, in addition, Torvinen discloses an interface for permitting an administrator to associate the location information to the edge device (Paragraph 40; associating a location-based group with edge devices, such as base stations, for example).

Regarding Claim 21,

Stewart as modified by Torvinen discloses the system of claim 10, in addition, Stewart discloses that the authentication server authenticates the identity (Column 9, lines 28-47; Column 12, line 30 to Column 13, line 10; Column 14, lines 40-56; Column 16, lines 38-55; and Column 18, lines 1-25).

Regarding Claim 22,

Stewart as modified by Torvinen discloses the system of claim 10, in addition, Stewart discloses that the authentication server includes a policy designating locations, if any, at which the client is permitted to connect to the network (Column 11, lines 28-53; and Column 16, lines 38-64); and Torvinen discloses that the authentication server (application server in some embodiments)

includes a policy designating locations, if any, at which the client is permitted to connect to the network (Paragraph 42).

Regarding Claim 24,

Stewart as modified by Torvinen discloses the system of claim 10, in addition, Stewart discloses that the identity includes information selected from the group consisting of a user name, a user password, a certificate, a MAC address, a shared key, a smart card identifier, and any combination of the foregoing information (Column 10, lines 53-63).

7. Claims 11, 20, 27-29, 31-37, 39-42, 45, and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Torvinen, further in view of Kwan (U.S. Patent Application Publication 2004/0255154).

Regarding Claim 11,

Stewart as modified by Torvinen does not explicitly disclose that the authenticator resides in a network switch.

Kwan, however, discloses that the authenticator resides in a network switch (Paragraph 56). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the multi-tiered network security system of Kwan into the distributed network access system of Stewart as modified by Torvinen in order to ensure that a client and its associated user are authentic and authorized to use the system by three levels of

security checks, including physical address authentication of the device, user credential authentication, and VLAN group association checks, thereby increasing security of the system.

Regarding Claim 20,

Stewart as modified by Torvinen does not explicitly disclose that the authentication server is included in a network switch.

Kwan, however, discloses that the authentication server is included in a network switch (Paragraph 36). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the multi-tiered network security system of Kwan into the distributed network access system of Stewart as modified by Torvinen in order to ensure that a client and its associated user are authentic and authorized to use the system by three levels of security checks, including physical address authentication of the device, user credential authentication, and VLAN group association checks, thereby increasing security of the system.

Regarding Claim 27,

Stewart discloses a network system comprising:

A plurality of edge devices capable of communicating with a plurality of user stations over one or more wireless channels (Figure 2; and Column 10, line 64 to Column 11, line 16);

One or more network switches (Figures 2-3; and Column 9, lines 52-64);

A first application for requesting station identities from the user stations and for associating corresponding location information with each of the station identities (Column 10, line 64 to Column 11, line 53);

An authentication server for deciding whether to grant or deny each of the user stations access to the network based upon the corresponding identity and location information (Column 9, lines 28-47; Column 12, line 30 to Column 13, line 10; Column 14, lines 40-56; Column 16, lines 38-55; and Column 18, lines 1-25);

A network that connects the authentication server and the one or more switches (Figures 1-3);

But does not explicitly disclose that the first application runs on the one or more network switches, a network manager comprising a server that runs an application that permits a network administrator to configure the location information and software images stored in the one or more switches, that the network manager either connects to the network or directly connects to the one or more switches and directly connects to the authentication server, or that when the network manager directly connects to the one or more switches and the authentication server, the network is bypassed.

Torvinen, however, discloses a network manager comprising a server that runs an application that permits a network administrator to configure the location information stored in the one or more switches (Figure 2; Paragraphs 27-28, 30, 42, 45, 48, 54, and 58); and

A network that connects the network manager, the authentication server, and the one or more switches (Figure 2; Paragraphs 27-28, 30, 42, 45, 48, 54, and 58);

Wherein the network manager either connects to the network or directly connects to the one or more switches and directly connects to the authentication server (Figure 2; Paragraphs 27-28, 30, 42, 45, 48, 54, and 58; as described above in the response to arguments);

Whereby when the network manager directly connects to the one or more switches and the authentication server, the network is bypassed (Figure 2; Paragraphs 27-28, 30, 42, 45, 48, 54, and 58; as described above in the response to arguments). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the conditional group access system of Torvinen into the distributed network access system of Stewart in order to allow various groups to be formed, by network operators and normal users alike, such that groups may be based upon the location of the device, device capabilities, user capabilities

or subscriptions, etc., thereby providing additional beneficial services to users by allowing them to communicate with other users that are in the same location and/or have the same interests.

Kwan, however, discloses that the first application runs on the one or more network switches, for requesting identities from user stations (Paragraph 56); and permitting a network administrator to configure software images stored in the one or more switches (Paragraphs 30, 42-46, and 53; updating information, functionality, and actions taken on/by the switch, for example). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the multi-tiered network security system of Kwan into the distributed network access system of Stewart as modified by Torvinen in order to ensure that a client and its associated user are authentic and authorized to use the system by three levels of security checks, including physical address authentication of the device, user credential authentication, and VLAN group association checks, thereby increasing security of the system.

Regarding Claim 28,

Stewart as modified by Torvinen and Kwan discloses the system of claim 27, in addition, Stewart discloses that at least one of the edge devices is a wireless access point (Figure 1; and Column 10, line 64 to Column 11, line 16).

Regarding Claim 29,

Stewart as modified by Torvinen and Kwan discloses the system of claim 27, in addition, Kwan discloses a user station that is a wired device for directly connecting to one of the ports of the one or more network switches (Figure 1; and Paragraph 35).

Regarding Claim 31,

Stewart as modified by Torvinen and Kwan discloses the system of claim 27, in addition, Stewart discloses that the location information indicates the location of one of the edge devices (Column 10, line 64 to Column 11, line 27).

Regarding Claim 32,

Stewart as modified by Torvinen and Kwan discloses the system of claim 27, in addition, Torvinen discloses an interface for permitting an administrator to associate the location information to the edge devices (Paragraph 40); and Kwan discloses that the network switch includes an interface for permitting an administrator to set information (Figure 2; element 210; and Paragraph 30).

Regarding Claim 33,

Stewart as modified by Torvinen and Kwan discloses the system of claim 27, in addition, Kwan discloses that the one or more network switches include an authenticator for authenticating the station identities (Paragraph 56).

Regarding Claim 34,

Stewart as modified by Torvinen and Kwan discloses the system of claim 27, in addition, Stewart discloses that the authentication server authenticates the station identities (Column 9, lines 28-47; Column 12, line 30 to Column 13, line 10; Column 14, lines 40-56; Column 16, lines 38-55; and Column 18, lines 1-25).

Regarding Claim 35,

Stewart as modified by Torvinen and Kwan discloses the system of claim 27, in addition, Stewart discloses that the authentication server includes a policy designating locations, if any, at which the user stations are permitted to connect to the network (Column 11, lines 28-53; and Column 16, lines 38-64).

Regarding Claim 36,

Stewart as modified by Torvinen and Kwan discloses the system of claim 27, in addition, Kwan discloses that the authentication server is a RADIUS server (Paragraphs 33 and 57).

Regarding Claim 37,

Stewart as modified by Torvinen and Kwan discloses the system of claim 27, in addition, Stewart discloses that the station identities include information selected from the group consisting of a user name, a user password, a certificate, a MAC address, a shared key, a smart card identifier, and any combination of the foregoing information (Column 10, lines 53-63).

Regarding Claim 39,

Stewart discloses a network system for controlling access to a network comprising:

Means for requesting an identity from a mobile client attempting to connect to the network (Column 10, line 64 to Column 11, line 16);

Means for receiving the identity (Column 10, line 64 to Column 11, line 16);

First associating means for associating location information corresponding to the client with the identity (Column 11, lines 17-53);

Authenticating means for authenticating the identity (Column 9, lines 28-47; Column 12, line 30 to Column 13, line 10; and Column 18, lines 1-25);

Means for comparing the location information against a policy designating locations, if any, at which the client is permitted to connect to the network (Column 11, lines 28-53; and Column 16, lines 38-64);

Means for deciding whether to grant or deny client access to the network based on the authenticity of the identity and comparison of the location information (Column 11, lines 28-53; Column 12, lines 47-63; and Column 16, lines 15-55);

A means for switching (Figures 2-3; and Column 9, lines 52-64); and

A network means that connects the means for authentication and the means for switching (Figures 1-3);

But does not explicitly disclose a means for network management comprising a means for a server that runs an application that permits a network administrator the means to configure the location information and software images stored in means for switching, that the network system further comprises a means for network management, wherein the means for network management configures the means for authenticating, that the means for network management either connects to the network or directly connects to the means for switching and directly connects to the means for authentication, and that when the means for network management directly connects to the means for switching and the means for authentication, the means for network is bypassed.

Torvinen, however, discloses a means for network management comprising a means for a server that runs an application that permits a network administrator the means to configure the location information stored in means for switching (Figure 2; Paragraphs 27-28, 30, 42, 45, 48, 54, and 58); and

A network means that connects the means for network management, the means for authentication and the means for switching (Figure 2; Paragraphs 27-28, 30, 42, 45, 48, 54, and 58);

Wherein the network system further comprises a means for network management, wherein the means for network management configures the means for authenticating (Figure 2; Paragraphs 27-28, 30, 42, 45, 48, 54, and 58);

Wherein the means for network management either connects to the network or directly connects to the means for switching and directly connects to the means for authentication (Figure 2; Paragraphs 27-28, 30, 42, 45, 48, 54, and 58);

Whereby when the means for network management directly connects to the means for switching and the means for authentication, the means for network is bypassed (Figure 2; Paragraphs 27-28, 30, 42, 45, 48, 54, and 58). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the conditional group access system of Torvinen into the distributed network access system of Stewart in order to allow various groups to be formed, by network operators and normal users alike, such that groups may be based upon the location of the device, device capabilities, user capabilities or subscriptions, etc., thereby providing additional beneficial services to users by allowing them to communicate with other users that are in the same location and/or have the same interests.

Kwan, however, discloses permitting a network administrator to configure software images stored in the one or more switches

(Paragraphs 30, 42-46, and 53). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the multi-tiered network security system of Kwan into the distributed network access system of Stewart as modified by Torvinen in order to ensure that a client and its associated user are authentic and authorized to use the system by three levels of security checks, including physical address authentication of the device, user credential authentication, and VLAN group association checks, thereby increasing security of the system.

Regarding Claim 40,

Stewart as modified by Torvinen and Kwan discloses the system of claim 39, in addition, Stewart discloses that the identity includes information selected from the group consisting of a user name, a user password, a certificate, a MAC address, a shared key, a smart card identifier, and any combination of the foregoing information (Column 10, lines 53-63).

Regarding Claim 41,

Stewart as modified by Torvinen and Kwan discloses the system of claim 39, in addition, Stewart discloses that the client is a wireless device capable of connecting to the network through an access point (Column 10, line 64 to Column 11, line 16).

Regarding Claim 42,

Stewart as modified by Torvinen and Kwan discloses the system of claim 39, in addition, Stewart discloses that the client is a wired device capable of connecting to the network through an Ethernet port (Column 5, lines 2-24; Column 6, lines 40-59; and Column 9, lines 48-64).

Regarding Claim 45,

Stewart as modified by Torvinen and Kwan discloses the system of claim 39, in addition, Stewart discloses that the location information indicates the location of an edge device for connecting the client to a network switch (Column 11, lines 17-27).

Regarding Claim 47,

Stewart as modified by Torvinen and Kwan discloses the system of claim 39, in addition, Stewart discloses that second associating means associates the mobile client with newly located access point upon authenticating the identity of the mobile client and determining, by comparing updated location information corresponding to the mobile client against the policy, that the mobile client is still authorized to access the network (Column 9, lines 28-47; Column 10, lines 25-37; Column 12, line 30 to Column 13, line 10; Column 14, line 57 to Column 15, line 15; and Column 18, lines 1-25).

8. Claims 17 and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Torvinen, further in view of Liming.

Regarding Claim 17,

Stewart as modified by Torvinen does not explicitly disclose that the location information indicates the location of a network switch to which the client is attempting to connect.

Liming, however, discloses that the location information indicates the location of a network switch to which the client is attempting to connect (Paragraph 159). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the location context system of Liming into the distributed network access system of Stewart as modified by Torvinen in order to allow the system to associate location information with the client even when the other devices cannot provide such location information, thereby extending the system to be able to be used when the client connects directly to a switch and/or when the other devices between the client and switch do not have any means to associate location information with the client.

Regarding Claim 49,

Stewart as modified by Torvinen and Liming discloses the system of claim 17, in addition, Liming discloses that the location information indicates the location of a port of a network switch to

which the client is attempting to connect (Paragraphs 159, 165, and 181).

9. Claims 23, 25, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Torvinen, further in view of Funk.

Regarding Claim 23,

Stewart as modified by Torvinen does not explicitly disclose that the authentication server is a RADIUS server.

Funk, however, discloses that the authentication server is a RADIUS server (Pages 1-6). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the AAA system of Funk into the distributed network access system of Stewart as modified by Torvinen in order to allow the system to centralize security and access controls, such as authentication, authorization, and accounting, manage the busiest of networks, scale to accommodate growing networks, and/or to provide high reliability and uptime.

Regarding Claim 25,

Stewart as modified by Torvinen does not explicitly disclose a network switch that comprises an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

Funk, however, discloses a network switch that comprises an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing (Page 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the AAA system of Funk into the distributed network access system of Stewart as modified by Torvinen in order to allow the system to centralize security and access controls, such as authentication, authorization, and accounting, manage the busiest of networks, scale to accommodate growing networks, and/or to provide high reliability and uptime.

Regarding Claim 26,

Stewart as modified by Torvinen does not explicitly disclose that the authentication server comprises an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

Funk, however, discloses that the authentication server comprises an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing (Page 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the AAA system of Funk into the distributed network access system of Stewart as modified by Torvinen in order to allow

the system to centralize security and access controls, such as authentication, authorization, and accounting, manage the busiest of networks, scale to accommodate growing networks, and/or to provide high reliability and uptime.

10. Claims 30 and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Torvinen and Kwan, further in view of Liming.

Regarding Claim 30,

Stewart as modified by Torvinen and Kwan does not explicitly disclose that the location information indicates the location of the one or more network switches.

Liming, however, discloses that the location information indicates the location of the one or more network switches (Paragraphs 159, 165, and 181). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the location context system of Liming into the distributed network access system of Stewart as modified by Torvinen and Kwan in order to allow the system to associate location information with the client even when the other devices cannot provide such location information, thereby extending the system to be able to be used when the client connects directly to a switch and/or when the other devices between the client and switch

do not have any means to associate location information with the client.

Regarding Claim 44,

Stewart as modified by Torvinen and Kwan does not explicitly disclose that the location information indicates the location of a network switch to which the client is attempting to connect.

Liming, however, discloses that the location information indicates the location of a network switch to which the client is attempting to connect (Paragraphs 159, 165, and 181). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the location context system of Liming into the distributed network access system of Stewart as modified by Torvinen and Kwan in order to allow the system to associate location information with the client even when the other devices cannot provide such location information, thereby extending the system to be able to be used when the client connects directly to a switch and/or when the other devices between the client and switch do not have any means to associate location information with the client.

11. Claims 38 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Torvinen and Kwan, further in view of Funk.

Regarding Claim 38,

Stewart as modified by Torvinen and Kwan does not explicitly disclose an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

Funk, however, discloses an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing (Page 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the AAA system of Funk into the distributed network access system of Stewart as modified by Torvinen and Kwan in order to allow the system to centralize security and access controls, such as authentication, authorization, and accounting, manage the busiest of networks, scale to accommodate growing networks, and/or to provide high reliability and uptime.

Regarding Claim 43,

Stewart as modified by Torvinen and Kwan does not explicitly disclose that the means for authentication includes an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

Funk, however, discloses that the means for authentication includes an authentication mechanism selected from the group

consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing (Page 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the AAA system of Funk into the distributed network access system of Stewart as modified by Torvinen and Kwan in order to allow the system to centralize security and access controls, such as authentication, authorization, and accounting, manage the busiest of networks, scale to accommodate growing networks, and/or to provide high reliability and uptime.

12. Claim 50 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Torvinen, further in view of Tan (U.S. Patent Application Publication 2001/0045451).

Stewart as modified by Torvinen does not explicitly disclose that the identity includes a smart card identifier.

Tan, however, discloses that the identity includes a smart card identifier (Paragraphs 20-23). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the smart card-based authentication techniques of Tan into the distributed network access system of Stewart as modified by Torvinen in order to provide multiple factor authentication, such that the user must first authenticate to the smart card, which will then allow the smart card to authenticate with the authentication server in a much more secure manner

than simply by sending a username and/or password to the server for authentication.

13. Claim 51 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Torvinen and Kwan, further in view of Tan.

Stewart as modified by Torvinen and Kwan does not explicitly disclose that the station identities include a smart card identifier.

Tan, however, discloses that the station identities include a smart card identifier (Paragraphs 20-23). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the smart card-based authentication techniques of Tan into the distributed network access system of Stewart as modified by Torvinen and Kwan in order to provide multiple factor authentication, such that the user must first authenticate to the smart card, which will then allow the smart card to authenticate with the authentication server in a much more secure manner than simply by sending a username and/or password to the server for authentication.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2437

/Jeffrey D Popham/
Examiner, Art Unit 2437